NUI Galway
OÉ Gaillimh

Semester 2 Examinations 2015/ 2016

Exam Code(s)	4BCT1, 1SWB1, 1OA1, 4BS2
Exam(s)	Year 4 BSc in Computer Science and Information Technology, Science without Borders, Occasional Students, Fourth Science
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Prof. G. Lyons Dr. J. Duggan *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	X	No	
MCQ	Yes		No	X

Handout	None
Statistical/ Log Tables	None
Cambridge Tables	None
Graph Paper	None
Log Graph Paper	None
Other Materials	None
Graphic material in colour	Yes [ ] No [X]

PTO

1

(a) Hash functions should be easy to compute and they should convert input of arbitrary size into a fixed-size output. In addition, they should provide three security properties: Pre-image resistance, second pre-image resistance and collision resistance. Explain what is meant by each of these security properties. (8 marks)

(b) A Message Authentication Code (MAC) differs from a hash function in that it has a symmetric key associated with it. In terms of security services, what in your view does a MAC provide that is not available with a hash function? (8 marks)

(c) Consider a digital signature scheme that involves a trusted arbitrator (A), a signer (S), and a verifier (V). A symmetric MAC key (K-SA) is shared by the signer and the arbitrator. Another such MAC key (K-AV) is shared between the arbitrator and the verifier. Sketch how a message should be transmitted from the signer to the verifier in such a scheme, and determine whether such a scheme can provide a non-repudiation service in the event that the signer S denies sending the message. (9 marks)

2

(a) 'A stream cipher can be viewed as performing bit-by-bit encryption on the plaintext using a keystream. Bit-by-bit decryption is then performed at the receiver.' By considering the expression Ci == Pi XOR Ki , where C is ciphertext, P is plaintext, K represents the keystream, XOR is exclusive-or, and i represents the current bit, explain how decryption works in such a scheme. (8 marks)

(b) In terms of strengthening a typical block cipher by introducing message dependency, outline how encryption and decryption work for the mode of operation known as Cipher Block Chain (CBC). (8 marks)

(c) 'A padding oracle attack is a very powerful way to attack a block cipher.' By considering an initialisation vector IV, and the first two blocks of ciphertext C1 and C2, explain how a padding oracle attack might work against an encryption service running in CBC mode. Assume that the blocksize is eight bytes. (9 marks)

3

(a) 'In order to provide an authentication service, one, two and three factor authentication can be employed for identifying an entity.' Explain what is meant by each of the terms 'one factor', 'two factor' and 'three factor' authentication. (8 marks)

(b) 'In addition to identifying an entity, in order to avoid replay attacks there should be some assurance of freshness in a communication. Freshness is often provided by a nonce.' Explain what is meant by the term 'nonce' and sketch how a nonce is employed to provide an assurance of freshness to a relying party. (8 marks)

(c) A bank uses a dynamic password scheme for authentication. Tokens (with keypads and screens) have been issued to customers. A customer accesses their bank account online. A challenge is issued to their mobile phone. Outline any one way such a scheme might operate, explaining the role of the challenge, the token and the response in the course of your answer. (9 marks)

PTO

4

(a) 'Public key encryption services such as RSA, ElGamal and Elliptic Curve rely on the apparent hardness of things like factorisation, extracting modulo roots, or solving a discrete log problem.' In terms of an RSA encryption service using public keys and private keys, explain in operational terms how a message is encrypted and decrypted, briefly explaining the terms 'Certification Authority' and 'Public Key Certificate' in the course of your answer. (8 marks)

(b) 'In connection with authentication, the fact that a man-in-the middle attack can succeed against Diffie-Hellman shows that a typical goal such as mutual entity authentication may not been achieved.' Outline how a protocol based on Diffie-Hellman such as STS (station-to-station) achieves mutual entity authentication by employing an established signature/verification key pair. (8 marks)

(c) 'Alice signs a draft message intended for Eve with her private signature key. She then encrypts the message with Bob's public encryption key and sends it to her assistant Bob for comment. Bob decrypts the message with his private decryption key and verifies that it came from Alice with Alice's public verification key. Bob then sends the message on to Eve directly using her public encryption key, pointing out numerous errors. The trust between Alice and Bob is abused here. Eve thinks that the message came from Alice (which it did), but that no-one else saw it (but Bob did).' Outline any one way that Alice could ensure that the draft status of her message to Eve is clear to all parties. (9 marks)

5

(a) In terms of computer forensics, explain what is meant by the term 'order of volatility' in the context of collecting computer evidence. (7 marks)

(b) 'Storage in the so-called 'Cloud' can lead to many problems for computer forensics.' By considering NISTIR 8006 Cloud Computing Forensic Science Challenges, or otherwise, outline any three challenges that you view as significant at this time. (9 marks)

(c) 'Steganography provides many challenges for forensic work, not the least of which is detecting it in the first place.' Give you understanding of the term 'steganography', discuss any one way you might attempt to detect its presence, and explain why the defence of plausible deniability is sometimes employed in connection with steganography. (9 marks)

6

'There is a balance to be struck between security and privacy. This is all the more so as we move into a world of devices and the Internet of Things.' By considering Landau's presentation to Congress on 1 March 2016, or otherwise, discuss this statement from the following three perspectives: Security threats (8 marks), encryption (8 marks), and securing devices such as smartphones (9 marks.)